ENTERPROTECT

WHITE PAPER

Cybersecurity: Understanding the Risks and Best Practices

Protect your organization from cyber threats with this comprehensive guide for executives.

WWW.ENTERPROTECT.COM

Disclaimer

Nothing contained in this document or relayed verbally will be deemed to amend, modify or supersede the Enterprotect Terms of Service or any other terms and conditions of any written agreement between the reader or reader's company and Enterprotect, or Enterprotect's subsidiaries or affiliates. Enterprotect does not make any promises or guarantees that any of the methods or suggestions described in this document will provide 100% protection against cybercrime, cyberattacks, disaster or similar incident. This document is not intended as legal advice nor should you consider it as such. The reader exclusively assumes all risk of utilizing or not utilizing any guidance described in this document.

ENTERPROTECT

Introduction

Cybersecurity is a critical concern for businesses of all sizes, as the threat of cyber-attacks continues to grow. It's been said, "nothing is certain but death, taxes and cyber threats", and it's more important than ever for organizations to take steps to protect themselves from these threats.

Cyber-attacks can come in many forms, such as malware, phishing, and ransomware. These attacks can have serious consequences, including financial loss, reputational damage, and the loss of sensitive data. Small and medium-sized organizations are particularly vulnerable to cyber-attacks, as they may not have the same resources or expertise as larger organizations to defend against them.

This report will provide a brief overview of the current state of cybersecurity threats and risks and will explain why it's crucial for small and medium-sized organizations to prioritize cybersecurity. It will also provide best practices for implementing robust cybersecurity measures and will conclude with a call to action for leadership to take the necessary steps to protect their organization from cyber-attacks. By understanding the importance of cybersecurity and taking the necessary steps to protect their organization, leadership can ensure the continued success and growth of their business.

Threats & Risks

In this section, we will discuss the common types of cyber-attacks that organizations face and the potential impact they can have. Cyber-attacks come in many forms, but some of the most common include:

- Malware: This is software that is designed to cause harm to a computer system. It can take many forms, such as viruses, worms, and Trojan horses. Malware can steal sensitive information, disrupt operations, or even destroy data. According to a report by Cybersecurity Ventures, a business will fall victim to a ransomware attack every 14 seconds by the end of 2019.
- Phishing: This is a type of social engineering attack in which an attacker poses as a trustworthy source and tries to trick the victim into providing sensitive information. This can be done through email, text message, or phone call. According to a report by Verizon, 30% of phishing emails are opened by the intended recipient and 12% of recipients open the attachment or click on the link.
- Ransomware: This is a type of malware that encrypts the victim's data and demands payment in exchange for the decryption key. This type of attack can cause significant disruption to business operations and can result in financial losses. According to a report by Cybersecurity Ventures, Ransomware damages will cost businesses $11.5 billion in 2019.

It's important to note that small and medium-sized businesses are particularly vulnerable to cyber-attacks. According to a report by the National Cyber Security Alliance, 60% of small and medium-sized businesses have experienced a cyber-attack. Additionally, of those businesses that have experienced a cyber-attack, 30% have reported financial losses as a result. These types of attacks can cause serious consequences, including financial loss, reputational damage, and the loss of sensitive data. The potential financial impact of a cyber-attack can be significant, and organizations may also face legal and regulatory consequences if they fail to protect sensitive data. Additionally, reputational damage can be difficult to recover from, as customers and partners may lose trust in an organization that has been compromised.

It is important for organizations to understand the risks and potential consequences of cyber-attacks, in order to prioritize cybersecurity and take steps to protect their assets and data.

The Importance of Cybersecurity

Small and medium-sized organizations may not have the same resources or expertise as larger organizations to defend against cyber-attacks. However, they are still a valuable target for cybercriminals due to the sensitive information they possess. A data breach or cyber-attack can have significant consequences for a small and medium-sized organization, including financial loss, reputational damage, and legal and regulatory penalties.

Furthermore, small and medium-sized organizations are increasingly subject to compliance requirements such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) which require them to implement robust cybersecurity measures to protect sensitive data. Failing to comply with these regulations can result in significant fines.

Implementing robust cybersecurity measures can also improve risk management for small and medium-sized organizations. By identifying and addressing potential vulnerabilities, organizations can reduce the likelihood and impact of a cyber-attack. Additionally, having a formal incident response plan in place can help organizations quickly and effectively respond to a cyber-attack, minimizing damage and reducing recovery time.

In summary, small and medium-sized organizations must prioritize cybersecurity to protect sensitive data, comply with regulations and improve risk management.

Best Practices for Cybersecurity

In this section, we will provide an overview of recommended cybersecurity measures for small to medium-sized organizations. These best practices can help organizations protect themselves from cyber-attacks and minimize the impact of a successful attack.

- Employee Training: Regular employee training on cybersecurity best practices, including how to identify and respond to potential threats, can significantly reduce the risk of a successful cyber-attack.
- Incident Response Planning: Having a formal incident response plan in place can help organizations quickly and effectively respond to a cyber-attack, minimizing damage and reducing recovery time.
- Vulnerability Management: Conducting regular vulnerability scans can help organizations identify vulnerabilities in their systems and take steps to address them before they can be exploited by cybercriminals.
- Network and Data Security: Implementing robust network and data security measures, such as firewalls, intrusion detection systems, and encryption can help protect sensitive data and prevent unauthorized access to your systems.
- 24/7 Monitoring and Response: Implementing 24/7 monitoring and having a dedicated team to respond to potential threats can help organizations detect and respond to cyber-attacks in real-time, minimizing damage and reducing recovery time.
- Automation and Tools: By equipping your IT team with the right tools and automation, you can proactively detect and eliminate vulnerabilities, persistent footholds on your systems, block known and zero-day threats, and ensure that your employees are protected against accidental exposure to malware or ransomware by visiting a malicious website or by clicking on a malicious link in an email.

Arming your IT team with the right tools and automation is crucial in protecting your organization from cyber-attacks. By equipping them with the necessary tools, they can proactively detect and eliminate vulnerabilities, persistent footholds on your systems, block known and zero-day threats, and ensure that your employees are protected against accidental exposure to malware or ransomware. It is also important to focus on preventative measures such as conducting regular vulnerability scans, implementing robust network and data security measures, and having a dedicated team for 24/7 monitoring and response. By implementing these best practices, your organization can significantly reduce the risk of a cyber-attack and minimize the impact of a successful attack.

ENTERPROTECT

Conclusion

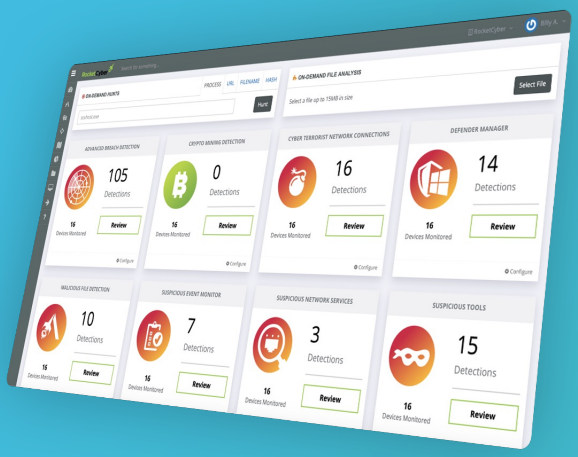
Cybersecurity is an ongoing concern for all organizations, and small to medium-sized businesses are particularly vulnerable to cyber-attacks. As the number of cyber threats continues to grow, it is essential for organizations to take proactive measures to protect themselves. In this report, we have outlined the risks and best practices for cybersecurity, including employee training, incident response planning, vulnerability management, network and data security, 24/7 monitoring and response, and equipping your IT team with the right tools and automation. By implementing these best practices, your organization can significantly reduce the risk of a cyber-attack and minimize the impact of a successful attack. It is important to remember that cybersecurity is not a one-time effort, but an ongoing process that requires constant attention and adaptation to evolving threats.

Introducing

ENTERPROTECT 360

The Cybersecurity Platform for Busy IT Professionals

Enterprotect 360 is an all-in-one solution that provides powerful protection across your endpoints, network, and cloud - monitored 24/7 by security experts and integrated into a single, easy-to-use console.



Protect Against Ransomware and Zero-day Threats
Multi-layer prevention, protection, detection, and response system stops emerging threats quickly with industry-leading efficacy.

Proactively Reduce Your Cyber Risk
Continuous scanning your endpoints, network, and internet-facing assets for vulnerabilities combined with simple-to-follow remediation guidance backed by support from security experts.

Detect and Eliminate Persistent Threats
Threat Hunting powered by real-time threat intelligence feeds detects, and eliminates, malicious footholds and persistent threats dwelling in your environment.

Add Cyber Experts to Your Arsenal
Extends your workforce with a team of security experts who reduce alert noise, review suspicious activity, and respond to security incidents 24/7.

Detect & Respond to Intrusions and Attacks Quickly
Real-time monitoring of malicious and suspicious activity, identifies attacker TTPs and triggers human response from the Security Operations Center 24x7.

Unified Cybersecurity Dashboard
Single, Cloud-based Cybersecurity Console lets you see all of your cybersecurity in one place, and provides easy access to alerts, tools and reports.

Try Enterprotect 360 including the 24/7/365 Security Operations Center

WWW.ENTERPROTECT.COM/FREE-TRIAL

ENTERPROTECT

Your Cybersecurity Partner

When it comes to cybersecurity, smaller IT teams have the toughest job out there. That's because you have to take care of everything IT-related - in addition to managing cybersecurity.

All too often, there is no one on your team dedicated to security – and even if there is, the bad guys don't clock out, and you/your security person can't work 24/7.

The choice seems to be - to go it alone - or try and get the budget to bulk up your security stack with more (often ineffective) cybersecurity tools.

That's why we created Enterprotect.

Enterprotect combines best-in-class technology and seasoned cybersecurity experts to make the job of managing cybersecurity much easier for smaller IT teams; without breaking the bank.

WWW.ENTERPROTECT.COM

Do you have feedback on this document?

Let us know what you think